Iowa Department of Administrative Services
Director's Office
Thomas J. Vilsack, Governor
Sally J. Pederson, Lt. Governor
Mollie K. Anderson, Director

State of Iowa Enterprise Information Security Policy

January 28, 2005

Purpose

The purpose of this Enterprise Information Security Policy is to create an environment within state of Iowa agencies that maintains system security and availability, data integrity and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to or loss of data. If there is a difference between this policy and other required policies, those with the more stringent control take precedence.

This document describes an enterprise level policy. Enterprise standards, processes and procedures will be developed to assist in the implementation. Each agency is responsible for developing policies, standards, processes and procedures to meet this policy. If it is determined that more stringent measures are needed, the agency is responsible for developing the policies, standards processes and procedures to meet that higher level of security.

General Policy Statement

Information is a state of Iowa asset requiring security commensurate with its value, criticality and sensitivity. The state is entrusted with this information and is accountable for its protection. Measures must be taken to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, and to ensure its authenticity, integrity and availability. When information is transferred either internally or externally to the State of Iowa information systems and networks, it must be protected from origin to destination.

Agency information technology processes, procedures, and practices may contain information (confidential or private) about the agency's business, communications, and computing operations or employees., Policies, standards, processes and procedures for distribution of any related documentation should consider both the sensitivity of the information and related statutory exemptions before public disclosure.

Availability of information systems and data resources must be maintained to ensure continued service to citizens and continuity of operations. Agencies must consider a security threat and guard against any action or inaction which interrupts the availability of information systems and data resources.

Hoover Building, Level A Des Moines, Iowa 50319 Phone (515) 281-5360 Fax (515) 281-6140

Scope

For the purposes of this policy, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by an agency. Security also involves the ability to protect information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction. In general, information technology assets covered by this policy include those that process, store, transmit or monitor digital information. It includes the security of information technology facilities and off-site data storage; computing, telecommunications and applications related services purchased from other state agencies or commercial entities; and Internet-related applications and connectivity.

This policy applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level security policies, standards, processes and procedures, as well as participate in enterprise level security programs.

Statutory Authority

Iowa Code Chapter 8A, Section 202, gives the Department of Administrative Services authorization for "Developing and maintaining security policies and systems to ensure the integrity of the State of Iowa's information resources and to prevent the disclosure of confidential records." The Department of Administrative Services is also responsible for "Prescribing standards and adopting rules relating to information technology and procurement, including but not limited to system design and systems integration and interoperability, which when implemented shall apply to all participating agencies except as otherwise provided in this chapter."

Compliance

All state of Iowa employees, interns, volunteers and contractors of participating agencies that use, develop, implement or maintain information technology systems covered by the enterprise information security policy are responsible for understanding and complying with all state of Iowa enterprise information security policies, standards, processes and procedures. This includes using, building, configuring and maintaining systems in accordance with these policies, standards, processes and procedures.

Depending on the severity, those who intentionally violate these policies, standards, processes and procedures may receive disciplinary action, up to and including loss of network connectivity, immediate dismissal and/or criminal prosecution.

On an agency level, non-compliant situations will be brought first to the attention of the agency and efforts will be made with the agency to bring it into compliance.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships and alliances, must be monitored and reviewed to ensure compliance with enterprise and departmental policies.

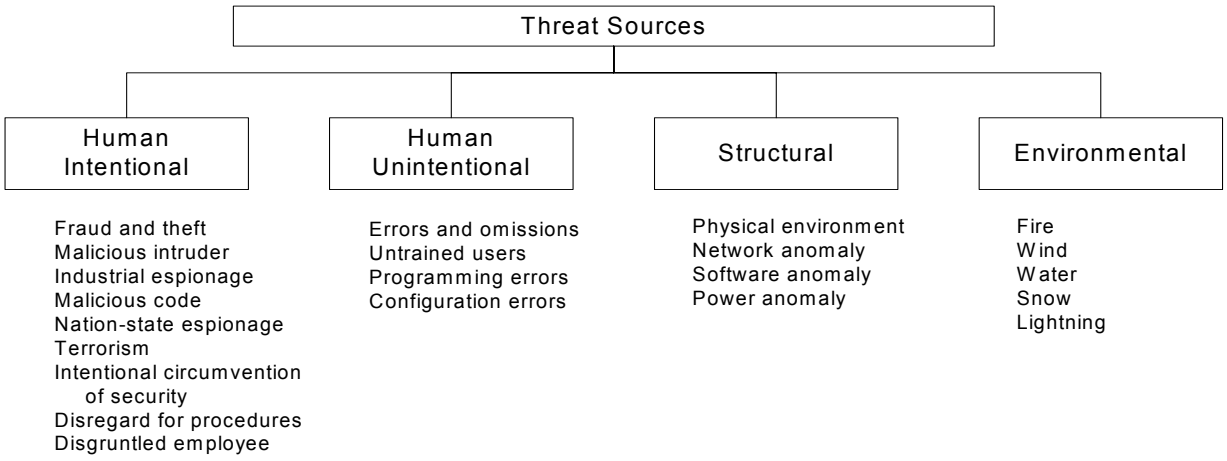
Agency directors may request exceptions to this policy. Requests must clearly explain the rationale and implications of the exception. The Chief Information Security Officer will either approve or deny the request within 15 days of submittal.

Updates

This document will be reviewed at least every two years and updated as needed.

Threats

State of Iowa information resources are vulnerable to many threats that must be considered when making risk management decisions. The potential impact of all threats should be considered when conducting a risk assessment. Threats can be categorized both by source and function. The following threats are representative and not all encompassing.



SECURITY PHILOSOPHY

Basic Principles

The basic security principles are to protect the confidentiality, integrity and availability of the information and information resources entrusted to the government of the State of Iowa.

- **Confidentiality** means that information deemed sensitive or confidential is protected and unavailable to those who do not have the necessary approvals to view it.
- **Integrity** means that information is correct and has not been altered or corrupted in some way. It also means that programs, applications, procedures and systems function as intended.

- **Availability** means that access to information and information systems is not denied to authorized users.

Security is an enabler critical to the success of technology initiatives and should not be viewed as a deterrent or irritant.

Information Assurance

Information security encompasses many disciplines, including computer security, network security, communications security and physical security. For Iowa state government systems, security will follow the concept of information assurance. The overall goal of information assurance is to protect and defend information and information systems. Disruptions in today's environment are not preventable 100 percent of the time; therefore, the state must be prepared to respond appropriately and recover to ensure the confidentiality, integrity and availability of its information and information systems. Information assurance entails information protection, event detection, appropriate response and restoration of information and services.

Defense in Depth

In the government of the state of Iowa, servers, PC's, networks, network components and other information technology devices will be implemented using the principle of "defense in depth."

Network and system security can be significantly improved when defense and detection measures are implemented in layers, so there are multiple opportunities to stop problems. This approach, in combination with an information assurance strategy, provides the best opportunity to reduce risks to appropriate levels.

Risk Management

It is impossible to eliminate all risk, but security measures are used to mitigate risk to acceptable levels, and all security decisions should be made with risk management in mind.

Access Control

Access control involves restricting physical access to resources and logical access to computers and networks. Access control decisions should be made based on the concept of least privilege, which means that individuals are given only those necessary accesses and rights, usually based on job duties and responsibilities.

Enterprise Information Assurance

State of Iowa agencies' computer systems and networks are increasingly interconnected, so a risk accepted by one agency is often a risk imposed on others. Therefore, an enterprise approach to

security with common security policies, standards, processes and procedures is needed. Security measures are most effective when considered end-to-end; that is, from the point of origin to the point of delivery.

ROLES AND RESPONSIBILITIES

Information assurance requires the active support and ongoing participation of all involved parties. It requires support from the executive level and universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with the development, implementation, operations, use and maintenance of government information systems. Each person shall satisfy the requirements as they relate to the portion of each information system under their control. Implementation, acceptance and maintenance of adequate system and network security is a shared responsibility of senior management, project managers, security and system administrators, supporting and using organizations, technology providers and users. Senior managers, project managers, technical staff and security personnel are responsible for evaluating the level of risk associated with any particular information system and implementing adequate security controls to reduce the risk to an acceptable level.

The following are specific roles and responsibilities both at the management and staff level.

Enterprise Information Security Office

Under the auspices of the Department of Administrative Services and under the leadership of the Chief Information Security Officer, the Information Security Office develops and implements an enterprise risk management program, publishes enterprise level security policies, standards, processes and procedures, and provides programs and processes to facilitate the implementation of this policy. The Information Security Office will serve as a central coordinating group to establish cyber security response procedures, ensure that best practices are shared, coordinate training and act as a catalyst to improve overall cyber security across state government.

It also coordinates the development of security service offerings and functions to ensure needed security services are available to Iowa government-related entities. The Chief Information Security Officer is responsible for maintaining a relationship with agencies; coordinating relevant information flow between the agency and the Information Security Office, and disseminating appropriate information throughout the Enterprise.

Agency Director

Agency directors (or equivalent), in coordination with their chief information officers and division administrators, are ultimately responsible for the implementation of the enterprise information security policy in their agencies and the development and implementation of agency security policies, standards, processes, and procedures. Agency directors also formally appoint primary and alternate agency security officers to function as liaisons to the Information Security Office.

Agency CIO

Each agency chief information officer coordinates with their director, security officer, and other management personnel to ensure the implementation of the enterprise information security policy. They also develop and implement agency security policies, standards, processes, and procedures. Each chief information officer is responsible for implementing an information technology program that includes security measures meeting or exceeding enterprise security policies, standards, processes and procedures.

Agency Security Officer

Each agency's security officer coordinates with the agency chief information officer and other management personnel to ensure the implementation of the enterprise information security policy in their agencies, including the development and implementation of agency security policies, standards, processes and procedures. The security officer is responsible for maintaining a relationship with the Information Security Office, coordinating relevant information flow between the agency and the Information Security Office, and disseminating appropriate information throughout the agency. The security officer is the Information Security Office's main point of contact within each agency.

Agency Managers/Supervisor

Managers and supervisors are responsible for ensuring their staff members know and understand appropriate security policies, standards, processes and procedures.

User

Each user shall, within his or her capabilities, protect information and system/network resources against occurrences of sabotage, tampering, denial of service, fraud, misuse or release of information to unauthorized persons. This includes protecting passwords and other account information; following appropriate policies, standards, processes and procedures; and notifying appropriate authorities when incidents occur.

Data Owner

Data owners (as defined by agency management) are responsible for authorizing access to data. Data owners approve all accesses to resources under their responsibility, judge the asset's value and label the data as such, and ensure compliance with applicable controls through regular review of data classification and authorized access. Data owners also assist in assessing the risks to the confidentiality, integrity and availability of applicable information and information resources.

System Administrator

The term "system administrator" is used here in the general sense, and includes system, network, firewall and other technology administrators that provide technical support to specific systems or networks. System administrators monitor performance, provide problem determination and production support and perform system back-ups. Security-related responsibilities include but are not limited to ensuring that:

- Applicable patches, service packs and updates are installed;
- Only authorized software is installed via authorized means;
- Systems are developed and implemented in a secure manner, following established enterprise security policies, standards, processes and procedures;
- Approved security procedures are followed and established where necessary;
- Systems are recovered in a secure manner;
- Ad hoc system reviews are performed to identify unusual activity;
- Security administrators are notified of changes to software that might impact system security features before installation of those changes; and,
- Procedures for software license validation and virus testing have been followed.

Security Administrator

Security administrators provide security-related administration tasks for critical systems. Where practical, separate system and security administration functions should exist; but in every case, both system and security administrative functions must be performed. When the system and security administration functions are performed by the same individual, care should be taken to ensure a secure approach is utilized. Security administration responsibilities include, but are not limited to:

- Development and implementation of system-specific security policies, standards, processes and procedures;
- Authentication (add, change, delete) services;
- Authorization (add, change, delete) services to provide access to applications;
- Generation and distribution of reports for monitoring access and potential security breaches; and,
- Developing incident handling procedures.

Database Administrator

Database administrators ensure the confidentiality, integrity, and availability of databases under their control. Security responsibilities include, but are not limited to:

- Designing, developing, organizing, managing and controlling databases in accordance with applicable security policies; and,
- Recovering databases in a secure manner when damaged or compromised.

Application Developer

Application developers develop secure applications consistent with established policies, standards, processes and procedures. Applications shall protect individual privacy, the confidentiality of electronic commerce information and the integrity of both the information it processes and the application itself. Applications must log significant security events, protect the log files appropriately and prevent co-mingling of data within the application.

ENTERPRISE INFORMATION SECURITY POLICY

It is the information security policy of the State of Iowa that:

1. Each agency operates in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of individual privacy and the assurance of data and business transactions. Each agency shall not jeopardize the confidentiality, integrity or availability of the state enterprise; or the information stored, processed and transmitted by any state information systems.

2. Each agency follows established enterprise security policies, standards, processes and procedures, except where agency policy provides a higher level of security.

3. Each agency is responsible for developing policies, standards, processes and procedures to meet this policy. If it is determined that more stringent measures are needed, the agency is responsible for developing the policies, standards processes and procedures to meet that higher level of security.

4. Each agency will develop, implement, and exercise an agency business continuity plan. The plan will be based on asset criticality and be consistent with the enterprise business continuity plan.

5. Each agency will implement a security awareness, training and education program for all staff including both technical and non-technical staff. The term "program" is intentionally used here. Each agency is expected to offer an on-going, systematic training program using a system-wide approach. Every new employee will be provided basic information technology security training within three months of employment. All employees, including interns, contractors, temporary and part-time employees, must agree in writing to follow state and agency security policies before being authorized to access state computer resources.

6. Each agency is subject to an annual security audit to assure compliance with this and other enterprise level policies, standards, processes and procedures. An audit or review performed under another authority, such as the Internal Revenue Service, may be substituted if similar in scope and approved by the Chief Information Security Officer.

7. Each agency will have a vulnerability assessment performed on its information systems at least annually to gauge the effectiveness of security measures. Assessment results may be used to identify, prioritize, plan for and implement additional security measures and to update the agency risk assessment.

8. Each agency will have an information systems risk assessment performed at least every two years. This assessment will be used to identify, prioritize, plan for and implement additional security measures. The assessment methodology will be developed by the Information Security Office and made available to the enterprise.

9. Security requirements will be formally defined and addressed throughout the life cycle of all information technology projects, including business requirements definition, design, development, testing, implementation and operation.

10. Each agency Chief Information Officer will assure to the best of his or her ability that information systems under their control meet enterprise and agency security policies, standards, processes and procedures prior to being placed in production or after significant changes to the system. The Information Security Office will randomly assess the self-certification process and individual systems to ensure adherence to policy.

11. All agencies will comply with appropriate federal information security requirements. However, if federal or other requirements are inconsistent with established state policy or standard, in whole or in part, then the Chief Information Security Officer may grant a waiver from the inconsistent portions of state policy or standard. Requests for a waiver must be submitted in writing and demonstrate that granting the waiver will not result in undue risk for the enterprise or agency.

12. Individual privacy will be protected at all times according to established laws, policies and rules.

13. Monitoring of information system usage for malicious activity and misuse of government resources will be conducted by agencies per their established policies, or by the Department of Administrative Services, the Iowa Communications Network or other party at the request of the agency.

14. Each agency will report network changes affecting enterprise network security to the Information Security Office.

15. Agencies will report information security incidents that impact or could impact shared resources to the Information Security Office, following a common response plan developed, implemented and exercised jointly by the Information Security Office and all agencies.

16. Computer resources and physical information, including but not limited to servers, desktops, laptops, network equipment, firewalls, hardcopies and tapes, have appropriate

physical protections in place. Where possible, these resources should also be protected from structural and environmental threats.

17. Agencies will provide information to the Information Security Office describing all connections from their agency networks to outside resources including the Department of Administrative Services shared campus network, the Iowa Communications Network, private service providers, federal, local and municipal governments and other state agencies. Updates will be provided as changes occur.

18. Agencies will develop procedures for implementing system patches, configuration updates, and other measures necessary to protect systems from known vulnerabilities. The procedures will provide for adequate testing prior to implementation to reduce the risk of a negative impact, but also assure the updates are applied quickly enough to assure protection.

19. Requests for exemption from any of the requirements of this policy will be submitted in writing by the agency director to the Chief Information Security Officer prior to implementation.